

# UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

DEVICE #1: Samsung, Galaxy A54 5G, 128 GB, bearing IMEI  
35312993063101.

)  
) Case No. 4:25-MJ-07066-SPM  
)  
) SIGNED AND SUBMITTED TO THE COURT FOR  
) FILING BY RELIABLE ELECTRONIC MEANS

## APPLICATION FOR A SEARCH WARRANT

I, Joel D. Bingaman, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed (*identify the person or describe the property to be seized*):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;  
 contraband, fruits of crime, or other items illegally possessed;  
 property designed for use, intended for use, or used in committing a crime;  
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

### Code Section - Offense Description

18 U.S.C. Sections 1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Conspiracy to Commit Fraud)

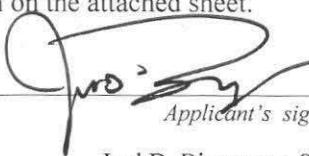
The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

Continued on the attached sheet.

Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.



Applicant's signature

Joel D. Bingaman, Special Agent

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures 4.1 and 41.

Date: 04/23/2025



Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Kyle T. Bateman

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI  
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:

**DEVICE #1:** Samsung, Galaxy A54 5G, 128  
GB, bearing IMEI 35312993063101.

No. 4:25-MJ-07066-SPM

SIGNED AND SUBMITTED TO THE  
COURT FOR FILING BY RELIABLE  
ELECTRONIC MEANS

**FILED UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41**  
**FOR A SEARCH WARRANT**

I, Joel D. Bingaman, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – electronic devices – described in Attachment A, and the extraction from that property of electronically stored information described in Attachment B.

2. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since April 2006. I am currently assigned to the FBI's St. Louis Division where I investigate complex financial crimes to include investigations of alleged criminal violations of Title 18, United States Code, Sections 1341, mail fraud, 1343, wire fraud, 1344 bank fraud and money laundering, including Sections 1956 and 1957. Prior to investigating

complex financial crimes, I was assigned to gang and narcotics investigations primarily focused on conspiracies associated with criminal offenses prohibited by Title 21, United States Code, Sections 841 and 846. Throughout my FBI career I have personally participated in investigations that involved the following techniques: questioning of witnesses; interviewing confidential human sources; conducting physical surveillance; conducting undercover operations which involved the purchase of drugs and/or other contraband; consensual and court authorized monitoring and recording of telephonic communications; gathering physical evidence, analyzing telephone pen registers and caller identification system data; analyzing data from mobile telephones and other electronic devices; and executing search warrants, seizure warrants and arrest warrants. I have also participated in numerous investigations involving money laundering and I am familiar with and have received training regarding the techniques employed by criminals to hide the proceeds derived from their illegal activities from detection by law enforcement. Throughout the course of my career, I have led and participated in numerous investigations to locate and apprehend fugitives from federal and state prosecutions to include fugitives that are charged with violations of Title 18, United States Code, Section 1073, unlawful flight to avoid prosecution. As a Federal Agent, I am authorized to investigate violations of the laws of the United States and to seek forfeiture of property under the authority of the United States.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Ronald Roberts (“Roberts”) and Kenneth Powell (“Powell”) and others known and unknown have committed violations of 18 U.S.C. Sections 1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Conspiracy to Commit Fraud) (“TARGET OFFENSES”). There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

**LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE**

6. The property to be searched is the following electronic devices (the “**subject cellular telephones**”):

**DEVICE #1:** Samsung, Galaxy A54 5G, 128 GB, bearing IMEI 35312993063101, in a purple and green case; and

**DEVICE #2:** Samsung Galaxy Z Flip, bearing IMEI 350258156245607.

7. The **subject cellular telephones** were seized from Roberts on April 18, 2025, upon his arrest pursuant to a federal arrest warrant related to the return of a Superseding Indictment by a Grand Jury in the Eastern District of Missouri. The **subject cellular telephones** are currently in the possession of the Federal Bureau of Investigation in the Eastern District of Missouri.

8. The applied-for warrant would authorize the forensic examination of the **subject cellular telephones** for the purpose of identifying electronically stored data particularly described in Attachment B.

### **TECHNICAL TERMS**

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth.
- b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24

NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- c. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- d. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication Devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions

and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

e. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

10. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available online, I know that the **subject cellular telephones** likely have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation Device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the **subject cellular telephones**.

#### **PROBABLE CAUSE**

11. On January 10, 2024, Roberts was charged with bank fraud and conspiracy to commit bank fraud, in violation of Title 18, United States Code, Section(s) 1344 and 1349, in

Case No. 4:24CR0013-RLW/RHH. Specifically, Roberts was charged with conspiring to defraud Simmons Bank between July 2019 and September 2022.

12. The investigation by the FBI revealed that Roberts and Powell (who was then an un-named co-conspirator) falsely represented to Victim 1 that they had a “contractual right” to purchase land in Baltimore, Maryland, that would result in a significant financial windfall to the victim investors. In truth and fact, there was no contractual right to purchase land in Baltimore, Maryland. Roberts and Powell told Victim 1 that a clause in the purported real estate contract required regular “earnings deposits” payments, typically in the amount of \$10,000 per week, to close the fictitious land deal.

13. Over the course of months, Roberts and Powell pressured Victim 1 on phone calls to provide additional cash funding under the false pretense that a purported imminent closing, often represented to be occurring within the next few days, could not occur unless or until such additional cash funds were received. As part of this pressure tactic, Roberts and Powell told Victim 1 that, if additional cash funds were not received in the short term, the closing would be pushed back further and would require even more cash funding in the future.

14. Roberts and Powell also falsely represented to Victim 1 that “Faulkenberry” is a wealthy man from Alabama who was helping to facilitate the deal by collecting payments and ensuring compliance with the “earnings deposits” clause. Roberts and Powell told Victim 1 on various occasions that “Faulkenberry” had shown them suitcases filled with cash.

15. When Victim 1 ran out of his own funds to cover the purported required “earnings deposit” payments, Roberts advised Victim 1 as to ways to obtain additional funds, including through borrowing from friends and family and/or taking out high interest rate personal or business loans.

16. Roberts and Powell received cash and cashier's checks from Victim 1 that he withdrew from his bank account at Simmons Bank and deposited them into various financial accounts, including ones held at Midwest Bank Centre in the Eastern District of Missouri.

17. As a part and result of the conspiracy, Roberts and Powell fraudulently obtained in excess of \$130,000 in funds from Victim 1, under the false pretenses, representations and promises described above.

18. On March 29, 2024, Roberts was arrested pursuant to a federal arrest warrant related to the Indictment described above. When Roberts was arrested, he had a single mobile phone on his person. This device was not seized and was left in the care of a friend of Roberts along with other personal items. One such item was Roberts' vehicle, a black Genesis sedan bearing Missouri license plate RK2H5V.

19. On March 29, 2024, Roberts was brought before United States Magistrate Judge Patricia Cohen for his Initial Appearance, Arraignment and Detention Hearing. As part of these hearings, Roberts signed a personal recognizance appearance bond, and he was released that day on bond.

20. Throughout that investigation, Roberts contacted victims utilizing telephone number 314-376-7815 to perpetrate the fraud scheme. Records received positive to the service of legal process determined that telephone number 314-376-7815, was associated to T-Mobile subscriber Ronald L. Roberts at 7016 Page Avenue, St. Louis, Missouri, beginning on or about April 1, 2020. 7016 Page Avenue is the location of PX Liquor, a business associated with Roberts.

21. In approximately September 2024, the FBI was contacted by Victim 2 claiming that he was a victim of a fraud scheme perpetrated by Roberts and Powell, and that he had recently provided cash to Roberts and Powell as part of that scheme.

22. In an interview with the FBI, Victim 2 advised that he was introduced to Powell by Roberts. Roberts and Powell then offered an investment opportunity to Victim 2 which was about to conclude in which Victim 2 would receive a large payout for helping a real estate deal get completed. The real estate deal, initially worth a few million dollars, was between Powell and a third party and involved a large plot of land located in South Carolina. For various reasons, the real estate deal could not be completed, and more investment money was required from Victim 2 to close the deal and get paid.

23. This pattern repeated continuously for many months and the value of the land deal increased to hundreds of millions of dollars. At some point, early on in the investment scheme, Victim 2 was introduced via telephone to “Nance”. “Nance” was a facilitator of the real estate land deal and was allegedly assisting both Roberts and Powell as well as the third party complete the deal. Victim 2 received many telephone calls from “Nance” throughout the course of investing in which “Nance” was coordinating for and with Roberts and Powell to convince Victim 2 to provide various amounts of cash in order to close the deal.

24. Ultimately, Victim 2 invested over \$2,000,000, all in cash, in which Victim 2 was subsequently promised to receive a \$175,000,000 payout when the deal closed. To date, the land deal has not closed and Victim 2 has not received any payout.

25. Victim 2 requested a refund of his investment but was told by Roberts, “Nance” and Powell that the money had already been spent and could not be returned.

26. Throughout the current investigation, and in fact previous investigations into Roberts criminal conduct of the same nature for which he was previously convicted for and served federal prison time for, it was also determined that Roberts utilizes a made-up persona(s) to further convince, coerce and defraud victims into investing in an alleged land deal promising a huge payout. In various incarnations, Roberts has pretended to be an individual serving the same role with slight name variations to include “Falkenberry,” “Falkenberg” and “Nance Falkenberg” (hereinafter Nance). This persona has been experienced by numerous victims and is generally described as a southern gentleman who serves as a facilitator, go-between and/or representative of the various iterations of a fictitious land deal. No one has ever met this persona in real life and the only contact is through telephone calls. On many occasions, “Nance” contacts the victims through a three-way call with Powell.

27. Despite the only method of contact between “Nance” and the victims being via telephone, none of the victims were ever provided with “Nance” telephone number and all calls received from “Nance” showed up as “No Caller ID” or some variation in which “Nance’s” telephone number was not identifiable to the victims. Generally speaking, if a user of a telephone dials ‘\*67’ before dialing the normal telephone number the caller identification feature will be disabled and the person receiving the telephone call cannot see the telephone number or subscriber information of the caller. Furthermore, when law enforcement reviews the telephone records for the person receiving such a telephone call, often times the records will show an incoming call and the duration of the call but will not contain the telephone number associated with person making the call.

28. A review of various telephone records received through the service of legal process over the past several years shows that Roberts, using telephone number 314-376-7815,

frequently dials ‘\*67’ before calling a subset of telephone numbers. These records show that Roberts, utilizing 314-376-7815, placed a large number of calls to Powell by first dialing ‘\*67’. Investigators believe this is a technique utilized by Roberts to conceal his activities from law enforcement and from victims.

29. On October 1, 2024, the FBI provided Victim 2 with \$3,000 to pay to Powell. This payment was requested by Roberts, Powell and “Nance” as a necessary investment payment to keep the land deal alive and to prevent Victim 2 from forfeiting all of the previous monies invested. CH was also provided with a recording device and Victim 2 subsequently met with Powell and provided him with the \$3,000 under the supervision of the FBI. Powell departed the meeting where he was paid by Victim 2 and was surveilled by the FBI as he drove to a fast-food restaurant where he parked and waited in his vehicle for over an hour for Roberts to show up. On the same day, and the days following, Victim 2 made several recordings of telephone calls with Roberts, Powell and “Nance” regarding the payment, the status of the ongoing land deal and their suspicion that Victim 2 was working with the FBI.

30. Through analysis of call log records received through the service of legal process, investigators were able to determine that subject telephone 314-376-9453 was likely associated to “Nance.” Subsequent analysis of call log records received through the service of additional legal process, and comparison to known call times of recorded conversations with victim CH, confirmed that “Nance” was utilizing 314-376-9453 to contact known victims to perpetuate the same fraud scheme along with Roberts and Powell. Records received positive to the service of legal process determined that telephone number 314-376-9453, was associated to Charter Communications subscriber Derick Jones at 10 Wayside Drive, Ferguson, Missouri from at least 1/1/2023 through 11/30/2024. Investigators believed Roberts was likely the actual user of 314-

376-9453 and possessed the telephone on a regular or permanent basis. Investigators further believe that Roberts uses Jones' as a straw subscriber to conceal his (Roberts) use of the telephone from law enforcement.

31. On March 3, 2025, precision location warrants were issued in Case No. 4:25-mj-03053 NCC and Case No. 4:25-mj-03054 for the aforementioned telephone numbers. Numerous physical surveillances were conducted based on the location data of the **subject cellular telephones** which showed that Roberts was in possession of both devices and was utilizing them on a regular basis to make telephone calls. For instance, Roberts is well known by investigators to frequent a barber shop known a Clippers and Shears located near the intersection of Jefferson Avenue and Cherokee Street. During several surveillances Roberts was observed to be at Clippers and Shears while precision location data for both subject telephones indicated that they were in the same area. Once Roberts was observed to depart the Clippers and Shears, precision location information for both devices no longer indicated that they were in the area and in fact continued to indicate that they were in the area that Roberts had moved to. Investigators followed Roberts on several occasions in which he appeared to aimlessly drive around St. Louis and surrounding areas. Precision location information for the subject mobile telephones showed that they were consistently located where Roberts was. Roberts was primarily observed driving a Genesis sedan bearing Missouri license plate RK2H5V that is registered to him. On one occasion Roberts was observed to be driving a dark Genesis SUV bearing Missouri license plate GL5X2A which is not a valid plate per the Missouri Department of Revenue. Additionally, on most days, precision location information for both devices indicated that the devices were located in the area of Robert's residence, 11557 Portsmouth Drive, St. Louis, Missouri, 63138

throughout the night into the early morning indicating that he was the sole possessor of both devices.

32. On April 16, 2025, a Grand Jury in the Eastern District of Missouri returned a Superseding Indictment charging the following: Roberts and Powell were charged with conspiracy to commit bank fraud (Count 1); Roberts was charged with bank fraud (Counts 2 and 3); Roberts and Powell were charged with conspiracy to commit wire fraud (Count 4); and Roberts was charged with wire fraud and committing crimes while on release (Count 5).

33. On April 18, 2025, utilizing precision location from the two devices, Roberts was observed departing his residence and traveling to “Clippers and Shears” where he was arrested by the FBI. Upon his arrest, agents seized both of the **subject cellular telephones** directly from Roberts’ hands. Additionally, after the **subject cellular telephones** were seized and subsequently turned off, the precision location data for each of the subject telephones stopped providing location information.

34. Most people that utilize a mobile phone typically upgrade and replace the device on a somewhat regular basis. Apart from bargain mobile phones, most people today utilize a smart phone which is a sophisticated device that is capable of performing many functions such as taking photos, sending and receiving email, providing directions, sending and receiving text and multimedia messages and accessing the internet. When a user upgrades a smart phone there is generally one or more processes in which the content stored on the existing smart phone is transferred to the new smart phone. Most smart phones operate on the Google Android or Apple IOS operating systems, While the exact process is different for each device and operating system, generally speaking, when user upgrades from a previous smart phone to a newer smart phone, the typical course of action is for the user to electronically transfer most of, if not all of,

the existing stored data from the older phone to the newer phone using one of the various methods provided. This data transfer allows a relatively seamless transition for the user as it does not require an intensive manual data entry process to store contact information and related data to the new device and users have access to previous communications, photos and other application data on the new device. Regardless of how the transfer is conducted, the end result is that the new phone will contain most of, if not all of, the data that the previous phone contained and for all intents and purposes, the new phone simply replaces the previous phone in form and function with minimal user effort. As many users upgrade their phones on a regular basis, if not yearly, a user's current phone may have data originally created on several different phones utilized by the user over many years. For this reason, and for the fact that Roberts was still utilizing the same telephone number that he utilized during the alleged commission of the target offenses, investigators believe that **subject cellular telephones** will have evidence of the target offenses despite Roberts potentially obtaining a new mobile phone, or phones, during the commission of the subject offenses.

35. In conclusion, your affiant believes that the **subject cellular telephones** will contain evidence of the target offenses and that the evidence will aid investigators in their ongoing criminal investigation and the continued identification of other victims.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

36. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

37. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Digital information on a computer, mobile phone, tablet, or other similar electronic media can be saved or stored on the device intentionally, i.e., by saving an e-mail as a file, or saving the location of one's favorite websites such as "bookmarked" or "favorite" files. Digital information can also be retained unintentionally, such as traces of the path of an electronic communication that may be automatically stored in many places (e.g., temporary files or internet Service Provider client software, among others). Applications operating on electronic devices also store data about the device user, times and locations of when an application may be operated by the user, and other data related to the general use of the application (such as a photo, a message, a search, etc.)
- c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal

information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

**CONCLUSION**

40. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

I state under the penalty of perjury that the foregoing is true and correct.



JOEL D. BINGAMAN  
Special Agent  
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 23rd day of April 2025.



HONORABLE SHIRLEY P. MENSAH  
United States Magistrate Judge

**SW 4:25-MJ-07066-SPM**

**ATTACHMENT A**

The property to be searched is the following electronic device (the “**subject cellular telephone**”):

**DEVICE #1:** Samsung, Galaxy A54 5G, 128 GB, bearing IMEI 35312993063101, in a purple and green case

1. The **subject cellular telephone** was seized from Roberts on April 18, 2025, upon his arrest pursuant to a federal arrest warrant related to the return of a Superseding Indictment by a Grand Jury in the Eastern District of Missouri. The **subject cellular telephone** is currently in the possession of the Federal Bureau of Investigation in the Eastern District of Missouri.

2. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

**SW 4:25-MJ-07066-SPM**

**ATTACHMENT B**

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. Sections 1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Conspiracy to Commit Fraud) (“TARGET OFFENSES”) from July 2019 to Present, including:

- a. Information that constitutes evidence concerning persons, including but not limited to Roberts and Powell, who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the **subject cellular telephones** about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
- b. Information that constitutes evidence indicating the **subject cellular telephones'** user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;
- c. Information related to the use of the aliases “Falkenberry,” “Falkenberg” and/or “Nance Falkenberg”
- d. Information related to communications with Victim 1, Victim 2, or any other individuals who were providing money to Roberts and/or Powell;
- e. Any information recording Roberts' schedule or travel from July 2019 to the present;
- f. All bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the **subject cellular telephones** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.